

Державний вищий навчальний заклад
Донецький національний технічний університет
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

_____Леонід БАЧУРІН

«_____» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДВС 1.03 ЗАХИСТ КОМП'ЮТЕРНИХ МЕРЕЖ

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність

125 Кібербезпека

(шифр і назва спеціальності (тей))

Освітня програма

Кібербезпека

(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни «Захист комп'ютерних мереж»
(повна назва дисципліни)

для здобувачів вищої освіти за спеціальністю 125 Кібербезпека «30» 08 2023 року. – 8 с.

Розробник:

Сергій ГІЛЬГУРТ, д.т.н., професор кафедри ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики

Протокол № 8 від “31” серпня 2023 р.

Завідувач кафедри прикладної математики та інформатики

_____ (Наталія МАСЛОВА)

“31” серпня 2023 р.

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології

Протокол № 5 від “ 1” 09 2023р.

Голова _____
(підпис)

(Євген БАШКОВ)
(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна
Статус	За вибором студента
Обсяг в кредитах ЄКТС	6
Обсяг в годинах за навчальним планом, разом: в тому числі:	180
лекції:	32
лабораторні заняття:	32
самостійна робота:	116
Форма підсумкового контролю	Екзамен
Дисципліну викладають	Викладач Д.т.н. Гільгурт С.Я., serhii.hilgurt@donntu.edu.ua , hilgurt@ukr.net

Передумови для вивчення дисципліни: перелік дисциплін, які мають бути вивчені раніше: Основи інформаційної безпеки, Системне програмування, Безпека та захист операційних систем, Теорія сигналів та процесів

2. Мета вивчення навчальної дисципліни

Метою вивчення навчальної дисципліни є опанування методами захисту комп'ютерних мереж, підготовка фахівців, здатних розробляти і використовувати технології захисту інформаційної та/або кібербезпеки.

Загальні компетентності:

- Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення захисту інформаційної та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
 - Здатність застосовувати знання у практичних ситуаціях.
 - Знання та розуміння предметної області та розуміння професії.
- ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- ФК 6. Здатність відновлювати штатне. Функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження
- ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
- ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
- ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки

Програмні результати навчання:

- ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
- ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур
- ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
- ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів
- ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах
- ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах
- ПРН50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
- ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах

3. Очікувані результати навчання

Результатами навчання є оволодіння практичними навичками з проведення процедур захисту комп'ютерних мереж.

В цілому результатами вивчення даної дисципліни є оволодіння методами та засобами забезпечення безпеки інформаційно-комунікаційних систем, підготовка фахівців, здатних розробляти і використовувати технології інформаційної та/або кібербезпеки.

4. Засоби діагностики результатів навчання

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Форма проведення поточного контролю – усна бесіда за результатами виконання практичних робіт.

Підсумковий контроль проводиться з метою оцінювання результатів навчання та визначається підсумками результатів виконання та захисту практичних робіт по кожній зі змістовних тем.

Підсумковий семестровий контроль – іспит.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Лр1	Лр 2	Лр 3	Лр 4	Лр 5	Лр 6	Лр 7	Лр 8	Поточний контроль	іспит	Максимальний бал
5	5	5	5	5	5	5	5	40	60	100
3	3	3	3	3	3	3	3	24		

Примітка: 1) Лр1, Лр2 і т.д. практичні роботи;

2) У чисельнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоєчасному виконанні)

В оцінку поточного контролю з виконання лабораторних робіт включено контрольні та поточні опитування

Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

5.1. Оцінка	
За 100-бальною шкалою	Для екзамену
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Тема 1. Безпека комп'ютерних мереж

Лекція 1. Основи безпеки сучасних мережевих систем

Тема 2. Міжмережеві екрани

Лекція 2. Класифікація міжмережевих екранів

Лекція 3. Мережеві фільтри, шлюзи, посередники

Лекція 4. Використання міжмережевих екранів

Лекція 5. Налаштування міжмережевих екранів

Тема 3. Сегментація мережі

Лекція 6. Сегментація мережі

Лекція 7. Віртуальні локальні мережі

Тема 4. Бездротові засоби зв'язку та їх безпека

Лекція 8. Технології цифрового бездротового зв'язку

Лекція 9. Безпека цифрових бездротових мереж

Лекція 10. Бездротові локальних мереж WiFi

Лекція 11. Безпека бездротових локальних мереж WiFi

Тема 5. Безпека мобільного зв'язку GSM

Лекція 12. Особливості мобільного зв'язку GSM та його захисту

Тема 6. Безпека телефонних мереж фіксованого зв'язку

Лекція 13. Особливості телефонних мереж та їх захисту

Тема 7. Безпека волоконно-оптичних ліній зв'язку

Лекція 14. Особливості передавання оптичного сигналу по ВОЛЗ

Лекція 15. Методи захисту ВОЛЗ

Тема 8. Грід та хмарні технології

Лекція 16. Безпека розподілених та хмарних обчислювальних технологій

6.2. Теми практичних (семінарських) занять

Проведення практичних занять не передбачено навчальним планом дисципліни

6.3. Теми лабораторних робіт

№ з/п	Назва теми	Кількість годин
1	Лабораторна робота №1 Налаштування міжмережевих екранів	4
2	Лабораторна робота №2 Міжмережеві екрани ОС Windows	4
3	Лабораторна робота №3 Сегментація мережі	4
4	Лабораторна робота №4 Безпека бездротових локальних мереж WiFi	4
5	Лабораторна робота №5 Безпека мобільного зв'язку GSM	4
6	Лабораторна робота №6 Безпека телефонної мережі	4
7	Лабораторна робота №7 Безпека волоконно-оптичних ліній зв'язку	4
8	Лабораторна робота №8 Безпека грід-мережі	4
	Усього годин	32

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Безпека комп'ютерних мереж	8
1.1	Лекція 1. Основи безпеки сучасних мережеских систем	8
2	Тема 2. Міжмережеві екрани	28
2.1	Лекція 2. Класифікація міжмережеских екранів	7
2.2	Лекція 3. Мережеві фільтри, шлюзи, посередники	7
2.3	Лекція 4. Використання міжмережеских екранів	7
2.4	Лекція 5. Налаштування міжмережеских екранів	7
3	Тема 3. Сегментація мережі	16

3.1	Лекція 6. Сегментація мережі	8
3.2	Лекція 7. Віртуальні локальні мережі	8
4	Тема 4. Бездротові засоби зв'язку та їх безпека	24
4.1	Лекція 8. Технології цифрового бездротового зв'язку	6
4.2	Лекція 9. Безпека цифрових бездротових мереж	6
4.3	Лекція 10. Бездротові локальних мереж WiFi	6
4.4	Лекція 11. Безпека бездротових локальних мереж WiFi	6
5	Тема 5. Безпека мобільного зв'язку GSM	8
5.1	Лекція 12. Особливості мобільного зв'язку GSM та його захисту	8
6	Тема 6. Безпека телефонних мереж фіксованого зв'язку	8
6.1	Лекція 13. Особливості телефонних мереж та їх захисту	8
7	Тема 7. Безпека волоконно-оптичних ліній зв'язку	16
7.1	Лекція 14. Особливості передавання оптичного сигналу по ВОЛЗ	8
7.2	Лекція 15. Методи захисту ВОЛЗ	8
8	Тема 8. Грід та хмарні технології	8
8.1	Лекція 16. Безпека розподілених та хмарних обчислювальних технологій	8
	Усього годин	116

6.5. Індивідуальні та/або групові завдання

У рамках курсу виконання індивідуальної науково-дослідної роботи не передбачено.

7. Література

7.1. Основна

1. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
2. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в КС від НСД
4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в КС від НСД
5. Бабак В.П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів // В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2013. – 670 с.
6. Юдін О.І. Захист інформації в мережах передачі даних // О.І. Юдін, О.Г. Корченко, Г.Ф. Конахович – К.: Вид-во ТОВ «НВП» Інтерсервіс», 2019. – 716 с.
7. William Stallings, Data and computer communications, Ninth Edition. – Prentice Hall, 2011. – 825 p.
8. Stallings W. Network Security Essentials: Applications and Standards. 4th Edition. – Prentice Hall, 2012. – 432 с.
9. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Київ, ЦП «Компринт», 2017 – 435 с.
11. Лосев Ю.І. Комп'ютерні мережі: навчальний посібник / Ю.І. Лосев, К.М. Руккас, С.І. Шматков / За редакцією Ю.І. Лосева. – Х. : ХНУ імені В.Н. Каразіна, 2013. – 248 с.
12. Інформаційна безпека в комп'ютерних мережах: навч. посіб. / О.А. Смірнов, О.К. Коноплицька-Слободенюк, С.А. Смірнов [та ін.]; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. – Кропивницький: Лисенко В.Ф., 2020. – 295 с.

7.2. Допоміжна

13. Мельников В.В. Захист інформації в комп'ютерних системах. – Фінанси й статистика, 1997. – 368 с.
14. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Захист інформації в комп'ютерних системах й мережах: Радіо і зв'язок, 1999. – 326 с.
15. Information technology. Security techniques. Information security management systems. Requirements, ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013.
16. Hilhurt S.Ya. Application of FPGA-based Reconfigurable Accelerators for Network Security Tasks // Simulation and informational technologies. Collection of scientific works of PIMEE of NAS of Ukraine. – Kyiv, 2014. – Vol. 73. – P. 17-26.
17. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
18. Hilgurt S. Parallel combining different approaches to multi-pattern matching for FPGA-based security systems / Serhii Hilgurt // Advances in Cyber-Physical Systems : scientific journal. – Lviv Polytechnic Publishing House, 2020. – Vol 5. – No 1. – P. 8-15. doi: 10.23939/acps2020.01.008.
19. Hilgurt S.Ya. A Survey on Hardware Solutions for Signature-Based Security Systems // Information Technologies: Theoretical and Applied Problems (ITTAP-2021): Proceedings of the 1st International Workshop, Ternopil, Ukraine, 16 – 18 Nov. 2021. – Ternopil: Faculty of Computer Information Systems and Software Engineering, 2021. – pp. 6-23. Available online: <https://ceur-ws.org/Vol-3039/paper17.pdf>.
20. Гільгурт С.Я. Метод прискореної кількісної оцінки компонентів реконфігуровних сигнатурних систем кіберзахисту // Електронне моделювання. – 2022. – Т. 44, № 5. – С. 3-24. doi: 10.15407/emodel.44.05.003.
21. Давиденко А.М., Гільгурт С.Я., Душеба В.В. Засоби додаткового захисту інформації користувачів у розподілених обчислювальних мережах // Проблеми інформатизації та управління. – Київ, 2022. – Том. 1, № 69. – С. 24-29, doi: 10.18372/2073-4751.69.16809.
22. Hilgurt S.Ya., Davydenko A.M., Matovka T.V., Prygara M.P. Tools for Analyzing Signature-Based Hardware Solutions for Cyber Security Systems // Journal of Cyber Security and Mobility. – 2023. – Vol. 12, No 3. – P. 339-366. <https://doi.org/10.13052/jcsm2245-1439.123.5>.

7.3. Методична

Методичні вказівки до виконання лабораторних робіт з дисципліни «Захист комп'ютерних мереж» для студентів денної форми навчання ОС «бакалавр» спеціальності 125 Кібербезпека (планується до видання).

8. Інформаційні ресурси

1. <https://www.lib.nau.edu.ua/>
2. <https://www.virtualbox.org/manual/>
3. <https://www.netacad.com/ru>
4. https://www.cisco.com/c/ru_ru/about/net-academy.html
5. <https://habr.com/ru/>